Remarks

Status of application

Claims 1-68 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

System providing methodology for access control with cooperative enforcement is described. In one embodiment, for example, a method of the present invention is described for authorizing a client to access a service based on compliance with a policy required for access to the service, the method comprises steps of: specifying a policy required for access to the service, the policy including security-relevant requirements that the client itself must meet (e.g., up-to-date antivirus software) before the client is provided access to the service; detecting a request for access to the service from the client; attempting authentication of the client based on credentials presented by the client; if the client is authenticated based on the credentials, determining whether the client is in compliance with the policy based, at least in part, on attributes of the client; and if the client is determined to be in compliance with the policy, providing access to the service.

General

The term "medium" has been changed to "storage medium" in claims 20, 56, and 68, as required by the Examiner.

Prior art rejections

A. Section 102 rejection: Moreh

Claims 1-68 stand rejected under 35 U.S.C. 102(e) as being anticipated by Moreh et al., US Patent Number 6,158,007, hereafter "Moreh." The Examiner's rejection of claim 1 is representative:

> As per claim 1, Moreh teaches a method for authorizing a client to access a service based on compliance with a policy required for access to

the service (col. 6 line 40 to col. 7 line 20), the method comprising: specifying a policy required for access to the service (col. 6 lines 4-20); detecting a request for access to the service from a client (col. 7 lines 1-11 and lines 39-60); attempting authentication of the client based on credentials presented by the client (fig 3 col. 7 lines 1-60); if the client is authenticated based on the credentials, determining whether the client is in compliance with said policy based, at least in part, on attributes of the client; and if the client is determined to be in compliance with said policy, providing access to the service (Moreh discusses compliance with policy on col. 4 lines 15-23).

For the reasons discussed below, Applicant's claimed invention is distinguishable over Moreh.

Moreh describes a security system for users to employ applications as either publishing applications or subscribing applications, for communicating messages on computer networks. (Moreh Abstract) As described by Moreh (at Moreh Col. 6, lines 7-17):

> The information 14 is in the form of messages 16 upon **subjects** 18 (FIG. 6), which each have a pre-defined security policy 20 stored in a security repository 22. The applications 12 may be either publishing applications 24 or subscribing applications 26, and each have an integrated client 28 (FIG. 3). The publishing applications 24 produce messages 16 classified by **subject** 18; the subscribing applications 26 register their interest in receiving these messages 16 by subscribing to the subjects 18; and a broker 30 working with the clients 28 of the applications 12 routes and handles the messages 16 according to the associated security policies 20 of the particular subjects 18. It is one of the inventors' key observations that the flow of information either inherently already depends upon classification by subject 18.

As shown above, the "predefined security policy" that Moreh discusses is a security policy pertaining to a subject of a message, such as "Subject: HR emp hire" (see, e.g., Moreh at Figs. 6 and 7). The security policy itself includes an access control list and a quality of protection. In this manner, Moreh is able to provide finer control over the communication of messages on a computer network.

Moreh's approach has little to do with Applicant's invention, as will now be explained. In Applicant's invention, a client is authorized to access a service based on the client's own compliance with a policy required for access to that service, such as a requirement that the client have up-to-date antivirus software or the requirement that the client be at a particular physical location (e.g., work PC, instead of a home PC). Thus, although both Applicant and Moreh use the terminology of "security policy," each is using the term in a different way, to describe different technology addressed at a different problem. In Moreh's case, the term "security policy" includes information pertaining to protecting the security of a given message based on its subject (heading). In Applicant's case, the term "security policy" is used to describe a policy that mandates client-specific requirements pertaining to protecting a given service (that may be accessed from client devices). Simply put, Moreh's security policy pertains to messages (based on subject) published or consumed by clients, while Applicant's security policy pertains to the individual clients themselves. As such, the two are fundamentally different approaches addressed at very different problems.

In order to appreciate these differences, consider the following example. Suppose a corporation wants to provide an Accounts Receivable service that is accessible by remote users (e.g., traveling salesman). In this example, the salesman may, after providing an appropriate username and password (i.e., after completing authentication), gain access to the service. However, suppose the salesman is accessing the service with a laptop computer that has been compromised with malware (i.e., malicious software), such as a virus or worm. In that case, even though the salesman has authenticated himself to the service, the device he is using may in fact be compromised such that it poses a risk to the entire corporate network (e.g., by uploading a worm, which then propagates to other computers on the network). Applicant's invention solves this problem by requiring, in addition to authentication information (i.e., user name and password), that the laptop

itself substantiate that it is in compliance with applicable security policies of the corporation (e.g., that it has up-to-date antivirus and firewall software). There is no reasonable way to argue that Moreh can also provide this solution. Moreh's security policy pertains to the subject of a message (e.g., "HR employee hire"), it does not pertain to the state of the underlying client machine itself that is generating the message. Thus, whether a given client machine in Moreh's system has up-to-date antivirus software or not is of no concern to the solution described by Moreh, which is addressed to making sure communication messages are secured (i.e., not read by inappropriate users).

It is appreciated that the Examiner's job is to read Applicant's claims with broad (or exceedingly broad) scope. In recognition of that and in order to expedite prosecution of the present application, Applicant's independent claims have been amended to better characterize the distinctions between Applicant's approach and that of Moreh. For example, Applicant's claim 1 has been amended to include the claim limitation of (shown in amended form):

> specifying a policy required for access to the service, the policy including security-relevant requirements that the client must meet before the client is provided access to the service;

Here, the amended claim makes it very clear that the recited "policy" pertains to security-relevant requirements that the client itself must meet before being granted access (to the requested service). This may include, for example, a policy mandating requirements about the client's antivirus software status, the client's endpoint protection (firewall) status, or the client's physical location (e.g., work PC, versus home PC, versus laptop connected to public WiFi network at Starbucks). Applicant's other independent claims have been amended in a like manner.

Moreh includes no discussion whatsoever pertaining to the security of individual clients, but instead focused his attention on securing messages. As such, it is respectfully submitted that Moreh does not teach or suggest Applicant's invention, as set forth in the amended claims. Accordingly, the amended claims distinguish over Moreh and are patentable under Section 102.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: January 26, 2009

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX